AMENDMENTS TO THE CLAIMS

1-6. (Canceled)

7. (New) A method of authenticating a user identity module communicatively coupled with a mobile shell having an established security association with a server network, the method comprising:

receiving a first message from the mobile shell;

determining a second message based upon the first message and a first key known to the server network and unknown to the mobile shell; and

providing the second message to the server network.

8. (New) The method of claim 7, wherein receiving the first message from the mobile shell comprises receiving the first message in response to a challenge interrogation message provided by the server network.

9. (New) The method of claim 8, wherein receiving the first message in response to the challenge interrogation message comprises receiving the first message from the mobile shell in response to at least one of a unique challenge interrogation message and a global challenge interrogation message.

10. (New) The method of claim 8, wherein receiving the first message comprises receiving a random number provided by the server network.

11. (New) The method of claim 10, wherein determining the second message comprises applying a non-reversible algorithmic function to the random number and the first key known to the server network and not known to the mobile shell.

12. (New) The method of claim 7, wherein receiving the first message from the mobile shell comprises receiving a first message formed by the mobile shell using a third message and a second key known to the mobile shell and the server network.

13. (New) The method of claim 12, wherein receiving the first message from the mobile shell comprises receiving the first message formed by the mobile shell using a third message and an integrity key known to the mobile shell and the server network.

14. (New) The method of claim 7, wherein providing the second message to the server network comprises providing the second message to the mobile shell, and wherein the mobile shell is configured to provide at least the second message to the server network.

15. (New) The method of claim 7, wherein determining the second message based upon the first key known to the server network and not known to the mobile shell comprises determining the second message based upon an anonymity key known to the server network and not known to the mobile shell.

16. (New) A method of authentication by a server network having an established security association with a mobile shell communicatively coupled with a user identity module, the method comprising:

establishing a security association with the mobile shell;

receiving a first message from the mobile shell; and

authenticating the mobile shell based upon the first message and a first key known to the user identity module and unknown to the mobile shell.

17. (New) The method of claim 16, wherein receiving the first message from the mobile shell comprises:

providing a second message to the mobile shell after the security association has been established; and

receiving the first message in response to the second message.

18. (New) The method of claim 17, wherein providing the second message comprises providing at least one of a unique challenge interrogation message and a global challenge interrogation message.

19. (New) The method of claim 17, wherein providing the second message comprises providing a random number.

20. (New) The method of claim 19, wherein receiving the first message comprises receiving a first message formed by the user identity module based upon the random number and the first key known to the user identity module and not known to the mobile shell.

21. (New) The method of claim 17, wherein authenticating the mobile shell based upon the first message and the first key known to the user identity module and not known to the mobile shell comprises:

B1

determining a fifth message based upon a portion of the second message and the first key known to the user identity module and not known to the mobile shell;

comparing the first message and the fifth message; and

authenticating the mobile shell when a portion of the first message is equal to a portion of the fifth message.

22. (New) The method of claim 21, wherein determining the fifth message comprises applying a non-reversible algorithmic function to the portion of the second message and the first key known to the user identity module and not known to the mobile shell.

23. (New) at the method of claim 16, wherein receiving the first message comprises receiving a third message formed by the user identity module based upon the first key and a fourth message formed by the mobile shell using a second key known to the mobile shell.

24. (New) The method of claim 23, wherein authenticating the mobile shell based upon the first message and the first key known to the user identity module and not known to the mobile shell comprises:

generating a sixth message based upon the first and second keys; and

comparing the first message and the sixth message; and

authenticating the mobile shell when a portion of the first message is equal to a portion of the sixth message.